How Attacks are Perpetrated Against Us

Todd Rector

Jared McLaren

Chris Rhodes

Paul Schmelzel

Why would someone want to attack State of Iowa resources?

- Chance - Hackers scan IP address ranges and the state network could happen to fall into the range
- Notoriety - We are a government site and hackers can deface us to put their name in the public eye to be noticed
- Control - Take control of our machines to attack other networks or machines and have it appear to come from the State of Iowa
- Political Motivation – people may disagree with things the State has done
  - Called Hactivists
- Theft or Misinformation - Our databases carry valuable information about citizens that hackers could steal or manipulate
- Email Abuse - Spammers look for open relays to bounce emails off of, and that can lead to the State being black listed

What are the most damaging attacks?

- Web page defacements because they are in the public’s eye
- Liability attacks
  - When hackers use State machines to attack other networks
- Worms
  - Take up bandwidth
  - Cause more strain on perimeter hardware
  - Cause Denial of Service on machines
  - If machines get infected there is downtime to rebuild
- The ones that we don’t know about!!

What are common security problems with regard to installing systems and programs?

- Default installs
  - Users don’t know what components get installed – for example, IIS on Windows 2000 server
  - Default applications – sample scripts get installed with IIS that can lead to easy server compromise
- Default passwords
  - Some are blank
  - Other defaults are well known
- People do not adhere to installation and security policy
  - Consultants may not know policy
- Downloads from the Internet
  - Freeware can contain viruses, Trojans, or spyware: scan before installing
- Need to install patches right when software is installed
  - Software out of the box probably already needs patches applied

What methods or tools can we use to detect attacks?

- MD5 checksums
- Netstat command to show connections to ports
- Logs – know a baseline
- Bandwidth usage
- Intrusion Detection System
- Know your system
  - What processes you run
  - Files that are on your machine
  - Normal usage

What methods or tools can we use to prevent attacks, or at least mitigate the risk or lessen the damage of attacks?

- Firewalls
- Backup - if affordable, keep two of everything so if a server must come down you have a replacement
- Install patches and stay current
- Know where you are getting your downloads from
- Change passwords (at least every sixty days)
- Use encryption
- Check logs as much as possible
- Keep anti-virus software up-to-date (update weekly)